REMARKS

This paper is responsive to a Non-Final Office action dated October 22, 2007. Claims 1-3, 5-16, 18-22, 26-35, 37-43, and 45-57 were examined. Claims 1-3, 5-8, 14-16, 18-22, 26, 27, 33-35, 37-39, 41-43, 45-51, and 53 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U. S. Patent Application Publication No. 2002/0094081 to Medvinsky (hereinafter, "Medvinsky"). Claims 9-13, 28-32, 40, and 52 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Medvinsky in further view of U.S. Patent No. 6,105,012 to Chang et al. (hereinafter, "Chang").

Information Disclosure Statement

Applicants request the Examiner to consider the references cited in the Information Disclosure Statement filed on March 24, 2003 and return an initialed copy of the substitute form 1449A/PTO.

Claim Rejections Under 35 U.S.C. § 102

Claims 1-3, 5-8, 14-16, 18-22, 26, 27, 33-35, 37-39, 41-43, 45-51, and 53 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U. S. Patent Application Publication No. 2002/0094081 to Medvinsky (hereinafter, "Medvinsky").

Claim 1 is amended to incorporate limitations of claim 54. The Office action admits that Medvinsky fails to teach

> padding an encrypted payload of the received data packet to a given size with padding, the given size corresponding to the fixed length segment size, and decrypting the payload of the received data packet by applying the fixed length segment of the continuous decryption key to the padded, encrypted payload, a portion of the fixed length segment being applied to the encrypted payload, a remaining portion of the fixed length segment being applied to the padding,

as required by amended claim 1. Accordingly, Applicants respectfully request that the rejection of claim 1, and all claims dependent thereon, as being anticipated by Medvinsky be withdrawn.

Claim 14 is amended to incorporate limitations of claim 55. The Office action admits that Medvinsky fails to teach

> padding data to generate padded data, applying the fixed length segment to the padded data to form padded encrypted data by applying a portion of the fixed length segment to the data to form an encrypted payload and applying a remaining portion of the fixed length segment to the padding, and de-padding the padded encrypted data to form the encrypted payload,

as required by amended claim 14. Accordingly, Applicants respectfully request that the rejection of claim 14, and all claims dependent thereon, as being anticipated by Medvinsky be withdrawn.

Regarding claim 33, Applicants respectfully maintain that Medvinsky, alone or in combination with other references of record, fails to teach or suggest

> a session count evaluator configured to determine if a difference between a received session count within a received encrypted data packet and a locally generated session count is less than a threshold,

as required by claim 33. In the Response to Arguments of the Office action mailed October 22, 2007, the Office states that those limitations of claim 33 are inherent in Medvinsky. Medvinsky teaches that

> [o]nce a secure channel is established, the process of exchanging voice packets is initiated. To begin, voice samples which are assembled into voice packets by MTA 104 are received. Thereafter, processor 124 coordinates with key stream generator 122 to begin generating a key stream based on a single key. Upon generation of the key stream, encryptor 118 encrypts each voice packet using the key stream. As noted, time stamps are employed to perform synchronization so the voice packets are recoverable at the remote end. Each voice packet includes an RTP time stamp used as a pointer to the key stream. Encryptor 118 employs the

> RTP time stamp to calculate an index into the key stream, and thereafter, calls key stream generator 122 to get the appropriate key stream bytes for encryption.
>
> Preferably, a stream cipher such as RC4 is employed although other comparable stream ciphers which require an external synchronization source may be used. In one embodiment, RC4 involves the XOR (Exclusive OR) of the voice packet bits and the key stream to produce encrypted data. After the encrypted data stream is received, processor 134 (of remote MTA 114) directs key stream generator 132 to output the same key stream bytes from the same key stream that was used to encrypt the voice packets at the local end. The key stream generator either generates the key stream bytes on-demand, or is free running based on the MTA clock and has the key stream bytes available by the time the RTP packet is received.

Paragraphs 0033-34 (emphasis added). The RTP time stamp of Medvinsky, which is used to calculate an index into a key stream, fails to teach the session count evaluator of claim 33. Applicants respectfully point out that while a teaching may be express or inherent, inherency is a stringent standard.

> To establish inherency, the extrinsic evidence "must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill." *Continental Can Co. v. Monsanto Co.*, 948 F.2d 1264, 1268, 20 U.S.P.Q.2D (BNA) 1746, 1749 (Fed. Cir. 1991). "Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient." Id. at 1269, 20 U.S.P.Q.2D (BNA) at 1749 (quoting *In re Oelrich*, 666 F.2d 578, 581, 212 U.S.P.Q. 323, 326 (C.C.P.A. 1981).

See *In re Robertson*, 169 F.3d 743, 745; 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999); MPEP § 2112.IV. Applicants disagree that it is inherent for the system of Medvinsky to practice the claim. For example, there is no teaching or suggestion that Medvinsky must (or does) include a session count evaluator configured to determine if a difference between a received session count within a received encrypted data packet and a locally generated session count is less than a threshold, as required by claim 33. To be inherent in including a session count evaluator as claimed, those functions must by necessity be performed in Medvinsky. They are not. Since Medvinsky fails to teach or suggest the limitations of claim 33, and no other reference provides the missing disclosure, Applicants respectfully request that the rejection of claim 33 be withdrawn.

Claim 41 is amended to incorporate limitations of claim 56. The Office action admits that Medvinsky fails to teach a transmitter including

> a padding engine configured to generate padded data, an encryption engine configured to apply a portion of a fixed length segment of a continuous encryption key stream to the padded data to form encrypted padded data, and a pad remover coupled to receive the encrypted padded data from the encryption engine and operable to remove the encrypted padding to generate a an encrypted payload,

as required by amended claim 41. Accordingly, Applicants respectfully request that the rejection of claim 41, and all claims dependent thereon, as being anticipated by Medvinsky be withdrawn.

Regarding claim 48, Applicants respectfully maintain that Medvinsky, alone or in combination with other references of record, fails to teach or suggest

> a session count evaluator configured to determine if a difference between a received session count within the encrypted data packet and a locally generated session count is less than a threshold,

as required by claim 48. In the Response to Arguments of the Office action mailed October 22, 2007, the Office states that those limitations of claim 48 are inherent in Medvinsky. Medvinsky teaches that

> [o]nce a secure channel is established, the process of exchanging voice packets is initiated. To begin, voice samples which are assembled into voice packets by MTA 104 are received. Thereafter, processor 124 coordinates with key stream generator 122 to begin generating a key stream based on a single key. Upon generation of the key stream, encryptor 118 encrypts each voice packet using the key stream. As noted, time stamps are employed to perform synchronization so the voice packets are recoverable at the remote end. Each voice packet includes an RTP time stamp used as a pointer to the key stream. Encryptor 118 employs the RTP time stamp to calculate an index into the key stream, and thereafter, calls key stream generator 122 to get the appropriate key stream bytes for encryption.

> Preferably, a stream cipher such as RC4 is employed although other comparable stream ciphers which require an external synchronization source may be used. In one embodiment, RC4 involves the XOR (Exclusive OR) of the voice packet bits and the key stream to produce encrypted data. After the encrypted data stream is received, processor 134 (of remote MTA 114) directs key stream generator 132 to output the same key stream bytes from the same key stream that was used to encrypt the voice packets at the local end. The key stream generator either generates the key stream bytes on-demand, or is free running based on the MTA clock and has the key stream bytes available by the time the RTP packet is received.

Paragraphs 0033-34 (emphasis added). The RTP time stamp of Medvinsky, which is used to calculate an index into a key stream, fails to teach the session count evaluator of claim 48. Applicants respectfully point out that while a teaching may be express or inherent, inherency is a stringent standard.

> To establish inherency, the extrinsic evidence "must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill." *Continental Can Co. v. Monsanto Co.*, 948 F.2d 1264, 1268, 20 U.S.P.Q.2D (BNA) 1746, 1749 (Fed. Cir. 1991). "Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient." Id. at 1269, 20 U.S.P.Q.2D (BNA) at 1749 (quoting *In re Oelrich*, 666 F.2d 578, 581, 212 U.S.P.Q. 323, 326 (C.C.P.A. 1981).

See *In re Robertson*, 169 F.3d 743, 745; 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999); MPEP § 2112.IV. Applicants disagree that it is inherent for the system of Medvinsky to practice the claim. For example, there is no teaching or suggestion that Medvinsky must (or does) include a session count evaluator configured to determine if a difference between a received session count within the encrypted data packet and a locally generated session count is less than a threshold, as required by claim 48. To be inherent in including a session count evaluator as claimed, those functions must by necessity be performed in Medvinsky. They are not. Since Medvinsky fails to teach or suggest the limitations of claim 48, and no other reference provides the missing disclosure, Applicants respectfully request that the rejection of claim 48 be withdrawn.

Claim 49 is amended to incorporate claim 50. Claim 50 is canceled. Regarding amended claim 49, Applicants respectfully maintain that Medvinsky, alone or in combination with other references of record, fails to teach or suggest that

> the selecting comprises selecting a current fixed length segment if a difference between the received session count and the locally generated session count is less than a threshold value,

as required by amended claim 49. The Office action apparently relies on paragraphs 0033-34 of Medvinsky to supply this teaching. Those portions of Medvinsky teach that

> [o]nce a secure channel is established, the process of exchanging voice packets is initiated. To begin, voice samples which are assembled into voice packets by MTA 104 are received. Thereafter, processor 124 coordinates with key stream generator 122 to begin generating a key stream based on a single key. Upon generation of the key stream, encryptor 118 encrypts each voice packet using the key stream. As noted, time stamps are employed to perform synchronization so the voice packets are recoverable at the remote end. Each voice packet includes an RTP time stamp used as a pointer to the key stream. Encryptor 118 employs the RTP time stamp to calculate an index into the key stream, and thereafter, calls key stream generator 122 to get the appropriate key stream bytes for encryption.
>
> Preferably, a stream cipher such as RC4 is employed although other comparable stream ciphers which require an external synchronization source may be used. In one embodiment, RC4 involves the XOR (Exclusive OR) of the voice packet bits and the key stream to produce encrypted data. After the encrypted data stream is received, processor 134 (of remote MTA 114) directs key stream generator 132 to output the same key stream bytes from the same key stream that was used to encrypt the voice packets at the local end. The key stream generator either generates the key stream bytes on-demand, or is free running based on the MTA clock and has the key stream bytes available by the time the RTP packet is received.

Paragraphs 0033-34 (emphasis added). The RTP time stamp of Medvinsky, which is used to calculate an index into a key stream, fails to teach selecting a current fixed length segment if a difference between the received session count and the locally generated session count is less than a threshold value, as required by amended claim 49. Since Medvinsky fails to teach or suggest the limitations of claim 49, and no other reference provides the missing disclosure, Applicants respectfully request that the rejection of claim 49 be withdrawn.

Claim Rejections Under 35 U.S.C. § 103 Over Medvinsky and Chang

Claims 9-13, 28-32, 40, and 52 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Medvinsky in further view of U.S. Patent No. 6,105,012 to Chang et al.

(hereinafter, "Chang"). Applicants believe that claims 9-13, 28-32, 40, and 52 depend from allowable base claims and are allowable for at least this reason. Accordingly, Applicants respectfully request that the rejections of claims 9-13, 28-32, and 40 be withdrawn.

Claim Rejections Under 35 U.S.C. § 103 Over Medvinsky and Sengodan

Claims 54-57 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Medvinsky in further view of U.S. Patent No. 6,918,034 to Sengodan et al. (hereinfter, "Sengodan"). Regarding amended claim 1, which incorporates limitations of claim 54, Applicants respectfully maintain that Medvinsky, alone or in combination with Sengodan, fails to teach or suggest

> padding an encrypted payload of the received data packet to a given size with padding, the given size corresponding to the fixed length segment size, and decrypting the payload of the received data packet by applying the fixed length segment of the continuous decryption key to the padded, encrypted payload, a portion of the fixed length segment being applied to the encrypted payload, a remaining portion of the fixed length segment being applied to the padding,

as required by amended claim 1. As discussed above with regard to the rejections under 35 U.S.C. § 102, Medvinsky fails to teach those limitations of amended claim 1. The Office action relies on Sengodan to supply this teaching. Sengodan teaches that "[t]he recipient after decrypting the mini-packet looks at the last byte 524 to determine the number of padding bytes 522 used." Col. 8, lines 19-21. Nowhere does Sengodan teach or suggest that the recipient pads any portion of a received data packet. Since Medvinsky and Sengodan fail to teach or suggest the recited limitations and no other art of record adds the missing disclosure, Applicants respectfully request that the rejection of amended claim 1 and all claims dependent thereon, be withdrawn.

Regarding amended claim 14, which incorporates limitations of claim 55, Applicants respectfully maintain that Medvinsky, alone or in combination with Sengodan, fails to teach or suggest

> padding data to generate padded data, applying the fixed length segment to the padded data to form padded encrypted data by applying a portion of the fixed length segment to the data to form an encrypted payload and applying a remaining portion of the fixed length segment to the padding, de-padding the padded encrypted data to form the encrypted payload, and combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet

as required by amended claim 14. As discussed above with regard to the rejections under 35 U.S.C. § 102, Medvinsky fails to teach those limitations of amended claim 14. The Office action relies on Sengodan to supply this teaching. Sengodan teaches

> assembling mini-packets into a payload wherein each mini-packet includes an associated mini-header for ensuring proper processing of each mini-packet and adding padding to mini-packets when the mini-packets are encrypted to insure each mini-packet is an integral multiple of a predetermined block size.

Col. 4, lines 30-36. Adding padding to mini-packets when the mini-packets of Sengodan are encrypted fails to teach or suggest generating padded data, forming padded encrypted data, de-padding the padded encrypted data to form the encrypted payload, and combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet as required by amended claim 14. Nowhere does Sengodan teach or suggest those limitations of amended claim 14. Since Medvinsky and Sengodan fail to teach or suggest the recited limitations and no other art of record adds the missing disclosure, Applicants respectfully request that the rejection of amended claim 14 and all claims dependent thereon, be withdrawn.

Regarding amended claim 41, which incorporates limitations of claim 56, Applicants respectfully maintain that Medvinsky, alone or in combination with Sengodan, fails to teach or suggest a receiver including

> a padding engine configured to generate padded data, an encryption engine configured to apply a portion of a fixed length segment of a continuous encryption key stream to the padded data to form encrypted padded data, a pad remover coupled to receive the encrypted padded data from the encryption engine and operable to remove the encrypted padding to generate an encrypted payload, and a session count generator configured to generate a packet number in accordance with the fixed length segment, the encrypted data packet comprising the encrypted payload and at least a portion of the session count,

as required by amended claim 41. As discussed above with regard to the rejections under 35 U.S.C. § 102, Medvinsky fails to teach those limitations of amended claim 41. The Office action relies on Sengodan to supply this teaching. Sengodan teaches

> assembling mini-packets into a payload wherein each mini-packet includes an associated mini-header for ensuring proper processing of each mini-packet and adding padding to mini-packets when the mini-packets are encrypted to insure each mini-packet is an integral multiple of a predetermined block size.

Col. 4, lines 30-36. Adding padding to mini-packets when the mini-packets of Sengodan are encrypted fails to teach or suggest a padding engine configured to generate padded data, an encryption engine configured to apply a portion of a fixed length segment of a continuous encryption key stream to the padded data to form encrypted padded data, a pad remover coupled to receive the encrypted padded data from the encryption engine and operable to remove the encrypted padding to generate an encrypted payload, the encrypted data packet comprising the encrypted payload and at least a portion of the session count, as required by amended claim 41. Nowhere does Sengodan teach or suggest those limitations of amended claim 41. Since

Medvinsky and Sengodan fail to teach or suggest the recited limitations and no other art of record adds the missing disclosure, Applicants respectfully request that the rejection of amended claim 41 and all claims dependent thereon, be withdrawn.

Claims 54-56 are canceled.

Regarding claim 57, Applicants respectfully maintain that Medvinsky, alone or in combination with Sengodan, fails to teach or suggest a receiver including

> a padding engine operable to pad an encrypted payload of the received encrypted data packet to generate the padded encrypted payload of the received encrypted data received by the decryption engine, a decryption engine configured to decrypt the padded encrypted payload of the received encrypted data packet by applying a portion of a current fixed length segment of a continuous decryption key stream to the padded encrypted payload to generate the padded decrypted data if the difference is less than the threshold, and a pad remover configured to remove padding from the padded decrypted data to recover the data,

as required by claim 57. The Office action admits that Medvinsky fails to teach those limitations of claim 57. The Office action relies on Sengodan to supply this teaching. Sengodan teaches that "[t]he recipient after decrypting the mini-packet looks at the last byte 524 to determine the number of padding bytes 522 used." Col. 8, lines 19-21. Nowhere does Sengodan teach or suggest that a receiver pads any portion of a received data packet. Since Medvinsky and Sengodan fail to teach or suggest the recited limitations and no other art of record adds the missing disclosure, Applicants respectfully request that the rejection of claim 57 and all claims dependent thereon, be withdrawn.

Additional Remarks

Claim 51 is amended to depend from claim 49.

In summary, all claims are believed to be allowable over the art of record, and a Notice of Allowance to that effect is respectfully solicited. Nonetheless, if any issues remain that could be more efficiently handled by telephone, the Examiner is requested to call the undersigned at the number listed below.

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that, on the date shown below, this correspondence is being

☐ deposited with the US Postal Service with sufficient postage as first class mail in an envelope addressed as shown above.

☐ facsimile transmitted to the USPTO.

☒ transmitted using the USPTO electronic filing system.

Nicole Teitler Cave — Date: 1/14/08

EXPRESS MAIL LABEL: _____

Respectfully submitted,

Nicole Teitler Cave, Reg. No. 54,021
Attorney for Applicant(s)
(512) 338-6315 (direct)
(512) 338-6300 (main)
(512) 338-6301 (fax)